明 細 書

情報の暗号化送受信方法

技術分野

[0001] 本発明はウェブネットワークに接続されたコンピュータを利用した様々な内容の平文情報の送受信において、送受信される情報が当該情報の送受信の当事者以外に解読されるおそれは全くない、完璧ともいえる暗号化送受信方法に関する。

背景技術

[0002] 従来から情報を暗号化して送受信する方法は、提案されている様々な暗号化方式によって行われている。このうち最もよく知られているRSA(Rirest—Shamir—Adleman)と呼ばれている暗号化方式は、受信者の「公開鍵」によって送信者の情報を暗号化して送信する一方で、これとは別途に送受信者がそれぞれの電子署名を互に送受信することにより、送信者の身元を受信者が確認し、送信情報が真正な送信者からのものであることを確認するという二重の手間を不可欠としている(例えば、特許文献1，2などを参照)。

特許文献1:特開平11—353280号公報

特許文献1:特開2001—052125号公報

発明の開示

発明が解決しようとする課題

[0003] 本発明は、送受信者の間で暗号化した情報をやり取りする送受信において、上記の公知暗号方式のように、送受信者の間で、別途に電子署名の送受信を行う必要がなく、従って、送受信者がお互に自分の鍵情報を相手に開示する必要がないのみならず鍵情報又はそれを用いた暗号化情報が第三者にきわめて解読され難いか乃至は事実上解読不能であるが、当事者は100%再現可能な暗号化送受信方法を提供することを課題とする。

課題を解決するための手段

[0004] 上記課題を解決することを目的としてなされた本発明暗号化送受信方法の構成は、ウェブネットワークを介して接続され互に送受信できるコンピュータを有する複数の

送受信者と、これらの送受信者が任意のビットデータにより夫々に形成した電子鍵のデータと各データに対応させたアドレスなどの個人データを前記の各送受信者からウェブネットワーク経由で受取って登録すると共に、前記の各個人データを各送受信者を認証するための認証データとするサーバーコンピュータを備えたデータセンターにより形成される適宜情報の送受信ネットワークにおいて、

送信者は受信者へ送信する平文などの原情報のビットデータを送信者の登録した電子鍵のビットデータにより排他的論理和処理し一次暗号化されたデータを前記送信者と受信者の個人データを付けて前記データセンターに送信する、

データセンターのサーバーコンピュータでは、一次暗号化されて送信されて来た送信情報のビットデータを前記送信者の個人データによって認証された当該送信者の電子鍵のビットデータにより排他的論理和処理することによって前記送信者の電子鍵のビットデータを除去すると共に、送信されて来た受信者の個人データによって認証された当該受信者の登録された電子鍵のビットデータにより排他的論理和処理して二次暗号化された送信情報のビットデータを作り当該受信者へ送信する、

データセンターからの二次暗号化された送信文のデータを受信した受信者は、そのビットデータを当該受信者の電子鍵のビットデータにより排他的論理和処理することによって前記二次暗号化された送信文のデータを、送信者から発信された平文などの原情報に復元する、

ことを第一の特徴とするものである。

[0005] 上記の本発明の暗号化送受信方法では、送信者と受信者とがウェブネットワーク上に設置したデータセンターを形成するサーバーコンピュータを介して直接繋っているため、送信者からの暗号送信が集中すると、いわば情報交通の渋滞状態を生じるおそれがある。

そこで本発明では、このような懸念を事前に払拭する目的で、次の構成を採ることとした。

即ち、ウェブネットワークを介して接続され互に送受信できるコンピュータを有する複数の送受信者と、これらの送受信者が任意のビットデータにより夫々に形成した電子鍵のデータと各データに対応したアドレスなどの個人データを前記の各送受信者

からウェブネットワーク経由で受取って登録すると共に各登録データを夫々の認証データとし、正当な照会者と認証できる者に対してのみ前記データを提供するサーバーコンピュータを備えたデータセンターにより形成される送受信ネットワークにおいて、

このウェブネットワークに接続されていて前記各送受信者における送信者のデータ送受信専用に設けた送信者専用のサーバーコンピュータと前記の各送受信者における受信者のデータ送受信専用に設けた受信者専用のサーバーコンピュータとを設置し、

送信者専用のサーバーコンピュータには、送信者が受信者に送る平文などの原情報のビットデータを自分の電子鍵のビットデータで排他的論理和処理して一次暗号化したデータが当該送信者と受信者の個人データを付けて送られる、

当該送信者専用サーバーコンピュータは、受信者の個人データをデータセンターに提示して認証を受け受信者の電子鍵のビットデータを受け取り、一次暗号化された前記ビットデータを、受け取った受信者の電子鍵のビットデータにより更に排他的論理和処理して二次暗号化し、これら送信者と受信者の個人データアを付けて受信者専用のサーバーコンピュータに送る、

二次暗号化されたビットデータを受取った受信者専用のサーバーコンピュータは、送信者の個人データをデータセンターに提示して認証を受け送信者の電子鍵のビットデータを受け取り、二次暗号化されたビットデータを受け取った送信者の電子鍵のビットデータにより排他的論理和処理して三次暗号化し、その旨を受信者に知らせるか、又は、三次暗号化されたデータを受信者に送る、

受信者は、三次暗号化されたビットデータを自分の電子鍵のビットデータにより排他的論理和処理することによって上記送信者から発信された平文などの原情報を得る、

ことを第二の特徴とするものである。

[0006] 本発明においてデータセンターのサーバーコンピュータでは、各送受信者が夫々に設定した電子錠のデータを前記の者を認証するための電子印鑑データとして利用すると共に前記送受信者の間で送受信するデータを情報隠蔽データとして用いる、

また、電子印鑑データと情報隠蔽データには、カオス画像データ又はフラクタル画像データを用いる。この画像データは動画データであることがなお好ましい。

[0007] このような特殊な画像データを用いる最大の理由は、カオス画像データ(静止画・動画)及びフラクタル画像データ(静止画・動画)ならば、後日、トラブル発生のために、法的(客観性ある)証拠として再演算が必要になった場合においても、本発明者は、純粋に数学理論に基づいてコンピュータ工学の常識を遥かに超越した演算精度を確保した解析可視化処理技術(近日中に特許出願予定)と、この処理技術の処理(プロセス・タスク)の流れを逆向きに活用した「不可視化処理技術」を相補系として、暗号化(エンコード)技術(不可視化処理技術)と復号(デコード)技術(可視化処理技術)として活用しているので、情報セキュリティの実用レベルでは100%の確度でデータを再現できることが保証されるからである。なおかつ、第三者が容易に同等画像データを生成できない演算ロジック(アルゴリズム)に基づく上記のような非線形反復演算型画像データを用いることにより、暗号強度及び証拠精度を極限まで高められるという長所を併せ持つからでもある。

[0008] また、本発明方法では、送信者が自分の電子鍵のビットデータで一次暗号化する平文などの原情報は、一次暗号化の前に、当該原情報のデータの少なくとも1バイトごとに、乱数ビットデータよって排他的論理和処理をして、予備暗号化し、このあと自分の電子錠のデータによって一次暗号化することもできる。この予備暗号化に用いた乱数ビットデータは、予備電子錠としてデータセンターのサーバーコンピュータに送信者の認証データと一緒に登録されると共に、認証された正当な受信者に提示される。

[0009] 本発明では、各電子鍵による各次の暗号化においても、上記予備暗号化と同様の手法で暗号化することができ、そうすることが望ましい。

また、上記の予備電子錠のデータは電子封筒のデータとして用いるようにしてもよい。

発明の効果

[0010] 本発明では、ウェブネットワーク上のデータセンターに各送受信者の電子鍵を夫々に登録しておき、このデータ-センターにおいて送信者が自分の鍵で暗号化した送

信文を、送信者の鍵を解いて受信者の鍵により暗号化するので、送受信当事者の認証と送信文の受信者向の暗号化とを同時に行うことができ、従って、公知の公開鍵方式のように、送信者の身元を受信者が確認するために不可欠であった送信者の電子署名を受信者に別途送信するという二度手間が不用になり、暗号文の送受信の高速処理化が可能になる。

また、送受信者間で、自分の鍵情報の送受信を行わないので、セキュリティの面でも優れている。

[0011] 即ち、本発明によれば、ウェブネットワーク上での情報のやりとりにおいて客観性のあるいわば法的証拠能力が、従来の「公証人役場」が関った書類のやりとりのように、いわば「デジタル公証人役場」における実印と割印が押捺されたとみなし得る（通信記録として残し得る）情報通信の移動過程（CR1⇒CR2⇒CR3）が介在するから、これによって電子署名の確認という従来型情報通信の「二度手間」が解消される。しかも従来型をはるかに上まわる客観性があるいわば法的認証機能（公証）を有した本発明の暗号化情報は、従来型の暗号化処理では必須であったトランプをシャッフルするような「情報の攪乱処理過程」をカオス画像（静止画・動画），フラクタル画像（静止画・動画）による情報の隠蔽〔電子印鑑（認め印あるいは実印）機能を有した特殊画像データと情報データとの排他的論理和〕に置き換えるので、本発明では公知の共通鍵型暗号に比べ短時間で公開鍵型暗号を上まわる客観性のある法的証拠能力を有しながらも「二度手間」を必要とせず、なおかつ、電子あぶり出し型暗号の長所をも併せ持った情報セキュリティネットワークシステムが構築できる。

発明を実施するための最良の形態

[0012] 次に本発明送受信方法の実施の形態例について図を参照して説明する。図1は本発明送受信方法の第二の構成における送受信システムと送受信態様を模式的に示したブロック図、図2は図1の本発明送受信方法における送信元と送信先の関係を説明するためのチャート図、図3は本発明送受信方法における平文，電子鍵，暗号文の各ビットデータの関係を説明するため、夫々のビットデータの一部を模式的に例示した説明図である。

[0013] 図1において、1はインターネットなどによるウェブネットワークである。このネットワー

ク1には、本発明送受信方法に使用する送受信者の電子鍵などの登録や本人確認などを行うためのメインサーバーコンピュータ2Aを具備したデータセンター2が接続されていると共に、複数の送信者又は受信者となるそれぞれにコンピュータを具備したユーザーが接続される。図1では、説明の便宜のため、コンピュータ3Aを具備した1人の送信者3と、同じくコンピュータ4Aを有する1人の受信者4を例示している。また、上記ウェブネットワーク1には、送信者の送受信に係る送信者専用のサーバーコンピュータ5(以下、送信者専用サーバー5ともいう)と受信者の送受信に係る専用のサーバーコンピュータ6(以下、受信者専用サーバー6ともいう)とが接続されている。

[0014] データセンター2のサーバーコンピュータ2Aは、送信者3と受信者4が、夫々の送信文, 受信文のデータを暗号化及び／又は復号化するための電子鍵のデータと夫々の住所などの個人データ、並びに、送受信者専用のサーバーコンピュータ5, 6のアドレスを登録し、サーバーコンピュータ2Aに登録された各データに照らし正当と認証された者からの請求に対して必要なデータを提供するようになっている。データセンター2のサーバーコンピュータ2Aへの前記各データの登録はビットデータによりなされる。

[0015] 電子鍵のデータと住所などの個人データをデータセンター2にそれぞれに登録した送信者3と受信者4は、ウェブネットワーク1に接続されたデータセンター2、並びに、夫々の送信者専用サーバー5と受信者専用サーバー6を介在して次の要領で暗号化した情報をやり取りするので、以下に説明する。以下の例では、送, 受信者の個人データは、送信者の便宜などに鑑み、住所データ(アドレス)としたが、本発明における個人データは、住所データ以外のデータであってもよい。

[0016] まず、送信者3は、送信したい平文情報のビットデータFDを自分の電子鍵のビットデータBPにより排他的論理和処理して一次暗号化し、一次暗号化したビットデータCR1を、このデータCR1に自分の住所データのタグ3adと受信者の住所データのタグ4adとを付けて、送信者専用サーバー5に送信する。

[0017] 送信者専用サーバー5では、受信した上記データの中の送信者のタグ3adと受信者のタグ4adをデータセンター2のサーバーコンピュータ2Aに送り、送信者3と受信者4について正当な者である認証を受け、受信者4がそこに登録している電子鍵のデー

タと受信者専用サーバー6のアドレスデータを入手する。そして、送信者専用サーバー5では、送信者から受信している一次暗号のデータCR1を、データセンター2から入手した受信者4の電子鍵のビットデータCSにより排他的論理和処理して二次暗号化し、二次暗号化したビットデータCR2を、このデータCR2に送信者の住所データのタグ3adと受信者の住所データのタグ4adを付けて受信者専用サーバー6に送信する。

[0018] 二次暗号化されたデータCR2を受信した受信者専用サーバー6では、送信者3の住所タグ3adをデーターセンター2のサーバーコンピュータ2Aに送って正当な者であることの認証を受け、サーバーコンピュータ2Aに登録されている送信者3の電子鍵のデータBPを入手し、このビットデータBPによって二次暗号化されたデータCR2を排他的論理和処理して三次暗号化したビットデータCR3を形成する。そして、この受信者専用サーバー6は三次暗号化したビットデータCR3が送信されたことを受信者4に通知する。この通知は、前記三次暗号化データCR3を直接受信者4に送付することを伴い行ってもよい。

[0019] 受信者4は、三次暗号化されたビットデータCR3の送信文を自分の電子鍵のビットデータCSにより排他的論理和処理をすると、前記の三次暗号化されているデータCR3は平文に戻るので、送信者3が送った平文情報を入手することができる。

[0020] 上記に説明した送信者3からの平文情報が、サーバーコンピュータ2A、送信者専用と受信者専用のサーバー5，6において暗号化されつつ受信者4に送られ、その受信者4の手元で平文化されるプロセスについて、図3に例示するビットデータの模式図を参照して説明する。図3の各ビットデータは本発明における暗号化と復号化を理解するのに足りるデータ量で示している。

[0021] 図3において、FDは平文を表わすビットデータの一部の例であり、このビットデータは無色が0、墨色が1を示すものとする。いま、平文のビットデータFDをその下に示した送信者3の電子鍵のビットデータBPにより排他的論理和処理すると、このデータBPの下に示した一次暗号化されたビットデータCR1が得られる。

[0022] 一次暗号化されたデータCR1を受信者4の電子鍵のビットデータCSでさらに排他的論理和処理すると、このデータCSの下に示した二次暗号化されたビットデータCR2が

得られる。

[0023] 次に、二次暗号化された上記データCR2を送信者3の電子鍵のビットデータBPにより排他的論理和処理すると、送信者の鍵のデータBPが除去された形の三次暗号化されたビットデータCR3が得られる。

[0024] そこで、三次暗号化された前記データCR3を受信者4の電子鍵のビットデータCSにより排他的論理和処理すると、三次暗号化されていたデータCR3は、受信者の電子鍵のデータCSが除去されて平文のビットデータFDに復号されるのである。

[0025] 以上の説明は、サーバーコンピュータを、データセンター2のサーバーコンピュータ2Aと、送信者専用のサーバコンピューター5，受信者専用のサーバーコンピューター6とに分けて、データセンター2の各サーバーコンピュータ2Aと夫々の専用サーバー5，6に夫々の役割を分担させる構成としたが、本発明暗号化送受信方法では、送信者と受信者の専用サーバーコンピューター5，6の役割を、データーセンター2のサーバーコンピュータ2Aに担わせることも可能である。

[0026] 以上に説明したように、本発明暗号化送受信方法では、

送信者3が自分の電子鍵のデータで一次暗号化処理をした情報をウェブネットワーク1を経て送信者専用のサーバーコンピュータ5に送信する、

送信者専用サーバーコンピュータ5はデータセンター2で認証を受けて一次暗号化された情報を二次暗号化処理してウェブネットワーク1を経て受信者専用のサーバーコンピュータ6に送信する、

受信者専用サーバーコンピュータ6ではデータセンター2の認証を受けて二次暗号化された情報を送信者3の電子鍵のデータで三次暗号化処理しウェブネットワーク1を経由して受信者4にその旨の連絡をするか、又は、三次暗号化処理された情報を受信者4に送信する、

受信者4は三次暗号化された情報を受け取り自分の電子鍵で復号化処理して平文に戻す、という手順を、データセンター2で認証局として作用するサーバーコンピュータ2Aを介して直列的に実行することにより、送信する情報の暗号化と認証とを同時不可分の関係で行っている。

従って、本発明送受信方法は公知RSA方式のように、送信者と受信者の間で電子

署名の送受信を行って送信者の正当性を確認する必要がなく、その手間が省ける。

[0027] しかし、本発明方法において、暗号鍵のデータにカオス画像又はフラクタル画像のデータ(静止画又は動画)を用いると、受信者4に送られて来た情報が、正しい情報なのか、ウィルスが紛れ込んだ情報なのか、改ざんされた情報なのか、なりすましによる情報なのか、単なるノイズであるのか、当該受信者は見分けられない。このため本発明では受信者専用のサーバーコンピュータ6に送信者3からメールが届いたことを、受信者4に画像又は画像と音声により形成されるいわば電子封筒機能により通知する。

[0028] 上記の電子封筒機能のためのビットデータは、本発明送受信方法のデータセンター2のサーバーコンピュータ2Aに、送信者3, 受信者4がその暗号鍵のデータを登録するとき、先に述べた個人データ(アドレスなど)の一つとして登録しておき、送信者3からの通信文のデータに添付されて受信者専用のサーバーコンピュータ6に送られ、このコンピュータ6から受信者4に電子封筒として送られるものである。この電子封筒機能のためのデータは、特定の送信者3と受信者4の共通鍵としてデータセンター2に登録することもできる。

産業上の利用可能性

[0029] 本発明は以上の通りであって、本発明の暗号化送受信方法では平文などの原情報と暗号化処理された情報のビット数が何段階に暗号化されても全く変化しないので、処理速度が早く、しかも、暗号化処理をいわば複合鍵により行うことなるので、安全強度が一層堅牢であるという利点がある。

[0030] 本発明方法では、鍵のデータにカオス画像データ又はフラクタル画像データであって、しかも動画データを用いると、鍵のデータを通信の度にではなく、例えば1/100秒などの微小時間単位で何度でも変えることができるので、第三者が不正を働くことが事実上不可能になるという特長がある。

[0031] また、上記の動画データを鍵のデータとして用いた暗号化された通信文が受信者に送付されることを予め電子封筒機能により受信者に知らせるので、受信者に送信された通信文が本発明の暗号化手法により高度に暗号化されたデータであっても、他のデータと混同したり、通信文が送られて来たことが判らないという問題は生じない。

図面の簡単な説明

[0032] [図1]本発明送受信方法の第二の構成における送受信システムと送受信態様を模式的に示したブロック図。

[図2]本発明送受信方法における送信元と送信先の関係を説明するためのチャート図。

[図3]本発明送受信方法における平文，電子鍵，暗号文の各ビットデータの関係を説明するため、夫々のビットデータの一部を模式的に例示した説明図。

符号の説明

[0033] 1 ウェブネットワーク

2 データセンター

2A データーセンターのサーバーコンピュータ

3 受信者

4 送信者

5 送信者専用のサーバーコンピュータ

6 受信者専用のサーバーコンピュータ

FD 平文情報のビットデータ

BP 送信者の電子鍵のビットデータ

CS 受信者の電子鍵のビットデータ

CR1 一次暗号化データ

CR2 二次暗号化データ

CR3 三次暗号化データ

請求の範囲

[1] ウェブネットワークを介して接続され互に送受信できるコンピュータを有する複数の送受信者と、これらの送受信者が任意のビットデータにより夫々に形成した電子鍵のデータと各データに対応させたアドレスなどの個人データを前記の各送受信者からウェブネットワーク経由で受取って登録すると共に、前記の各個人データを各送受信者を認証するための認証データとするサーバーコンピュータを備えたデータセンターにより形成される適宜情報の送受信ネットワークにおいて、

送信者は受信者へ送信する平文などの原情報のビットデータを送信者の登録した電子鍵のビットデータにより排他的論理和処理し一次暗号化されたデータを前記送信者と受信者の個人データを付けて前記データセンターに送信する、

データセンターのサーバーコンピュータでは、一次暗号化されて送信されて来たビットデータを前記送信者の個人データによって認証された当該送信者の電子鍵のビットデータにより排他的論理和処理することによって前記送信者の電子鍵のビットデータを除去すると共に、送信されて来た受信者の個人データによって認証された当該受信者の登録された電子鍵のビットデータにより排他的論理和処理して二次暗号化されたビットデータを作り当該受信者へ送信する、

データセンターからの二次暗号化されたビットデータを受信した受信者は、そのビットデータを当該受信者の電子鍵のビットデータにより排他的論理和処理することによって前記二次暗号化されたビットデータを、送信者から発信された平文などの原情報に復元する

ことを特徴とする情報の暗号化送受信方法。

[2] ウェブネットワークを介して接続され互に送受信できるコンピュータを有する複数の送受信者と、これらの送受信者が任意のビットデータにより夫々に形成した電子鍵のデータと各データに対応したアドレスなどの個人データを前記の各送受信者からウェブネットワーク経由で受取って登録すると共に各登録データを夫々の認証データとし、正当な照会者と認証できる者に対してのみ前記データを提供するサーバーコンピュータを備えたデータセンターにより形成される送受信ネットワークにおいて、

このウェブネットワークに接続されていて前記各送受信者における送信者のデータ

送受信専用に設けた送信者専用のサーバーコンピュータと前記の各送受信者における受信者のデータ送受信専用に設けた受信者専用のサーバーコンピュータとを設置し、

送信者専用サーバーコンピュータには、送信者が受信者に送る平文などの原情報のビットデータを自分の電子鍵のビットデータで排他的論理和処理して一次暗号化したビットデータが当該送信者と受信者の個人データを付けて送られる、

当該送信者専用サーバーコンピュータは、受信者の個人データをデータセンターに提示して認証を受け受信者の電子鍵のビットデータを受け取り、一次暗号化された前記ビットデータを、受け取った受信者の電子鍵のビットデータにより更に排他的論理和処理して二次暗号化し、これら送信者と受信者の個人データを付けて受信者専用サーバーコンピュータに送る、

二次暗号化されたビットデータを受取った受信者専用サーバーコンピュータは、送信者の個人データをデータセンターに提示して認証を受け送信者の電子鍵のビットデータを受け取り、二次暗号化されたビットデータを受け取った送信者の電子鍵のビットデータにより排他的論理和処理して三次暗号化し、その旨を受信者に知らせるか、又は、三次暗号化されたビットデータを受信者に送る、

受信者は、三次暗号化されたビットデータを自分の電子鍵のビットデータにより排他的論理和処理することによって上記送信者から発信された平文などの原情報を得ることを特徴とする情報の暗号化送受信方法。

[3] 送信者が自分の電子鍵のビットデータで一次暗号化する平文などの原情報は、一次暗号化の前に、当該原情報のデータの少なくとも1バイトごとに、乱数ビットデータよって排他的論理和処理をして、予備暗号化する請求項1又は2の暗号化送受信方法。

[4] 乱数及び／又は電子鍵のビットデータは、64進数6桁ー10桁の数を含むn進数の数によるパスワード乱数乃至当該乱数に基づく擬似乱数、又は、カオス乱数、若しくは、フラクタル乱数である請求項3の暗号化送受信方法。

[5] サーバーコンピュータのデータセンターは、各送受信者が夫々に設定した電子錠のデータを前記の者を認証するための電子印鑑データとして利用すると共に前記送

受信者の間で送受信するデータの情報隠蔽データとして用いる請求項1ー4のいずれかの暗号化送受信システム。

[6] 請求項5の電子印鑑データ及び／又は情報隠蔽データには、カオス画像データ又はフラクタル画像データを用いる請求項5の暗号化送受信システム。

[7] 請求項6の画像データは、動画データである請求項6の暗号化送受信システム。

[8] 受信者には、暗号化された通信文が送られて来たことを電子封筒のデータにより受信者専用のサーバーコンピュータが通知する請求項2ー7のいずれかの暗号化送受信システム。

[9] 送信したい平文などの原情報のビットデータ(ア)を、そのデータ(ア)の任意数のバイトごとに、送受信者がともに知っている乱数ビットデータ(イ)により排他的論理和処理して一次暗号化したデータ(ウ)を形成する、

送信者又は送受信者のみが入手できる電子鍵のビットデータ(エ)により前記データ(ウ)を排他的論理和処理して二次暗号化したデータ(オ)を形成する、

受信者又は送受信者が登録した電子封筒のビットデータ(カ)により前記データ(オ)を排他的論理和処理して三次暗号化したデータ(キ)を形成する、

前記電子封筒のデータ(カ)とともに三次暗号データ(キ)を受信者に送信することを特徴とする暗号化送受信方法。

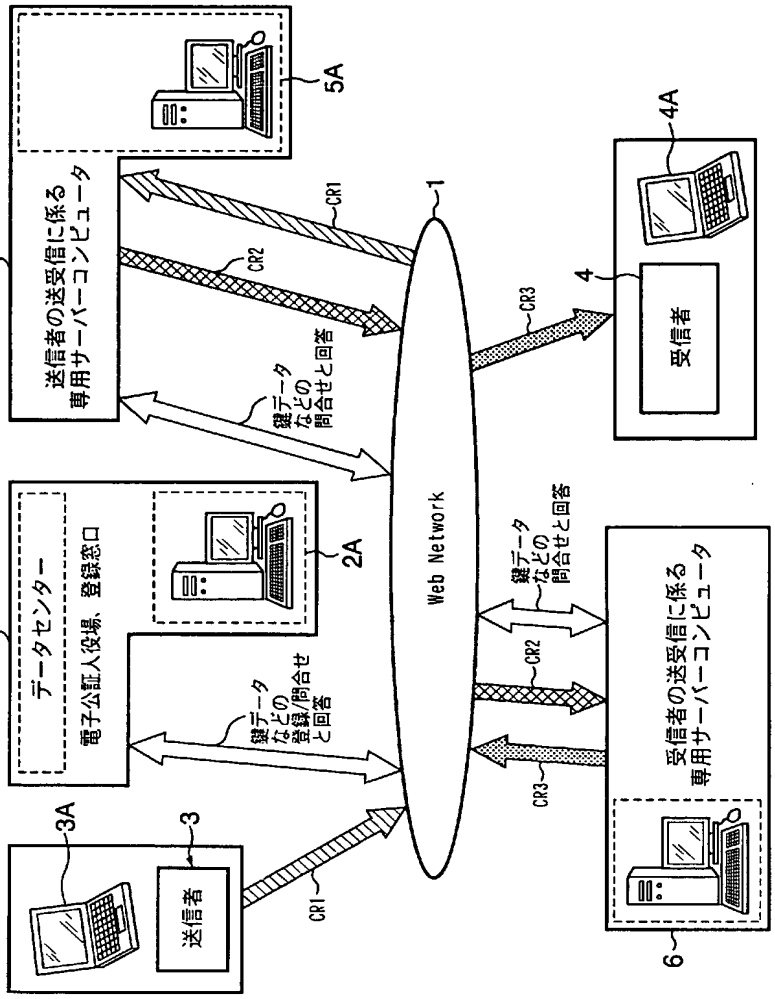
[10] 乱数のビットデータ、電子鍵のビットデータ、電子封筒のビットデータはデータセンタ

乃至認証局として設定されるサーバーコンピュータに正当な者のみが読出し可能に登録する請求項8の暗号化送受信方法。

[11] 乱数及び／又は電子鍵のビットデータは、64進数6桁ー10桁の数を含むn進数の数によるパスワード乱数乃至当該乱数に基づく擬似乱数、又は、カオス乱数、若しくは、フラクタル乱数である請求項9又は10の暗号化送受信方法。

WO 2005/039102 PCT/JP2004/015493

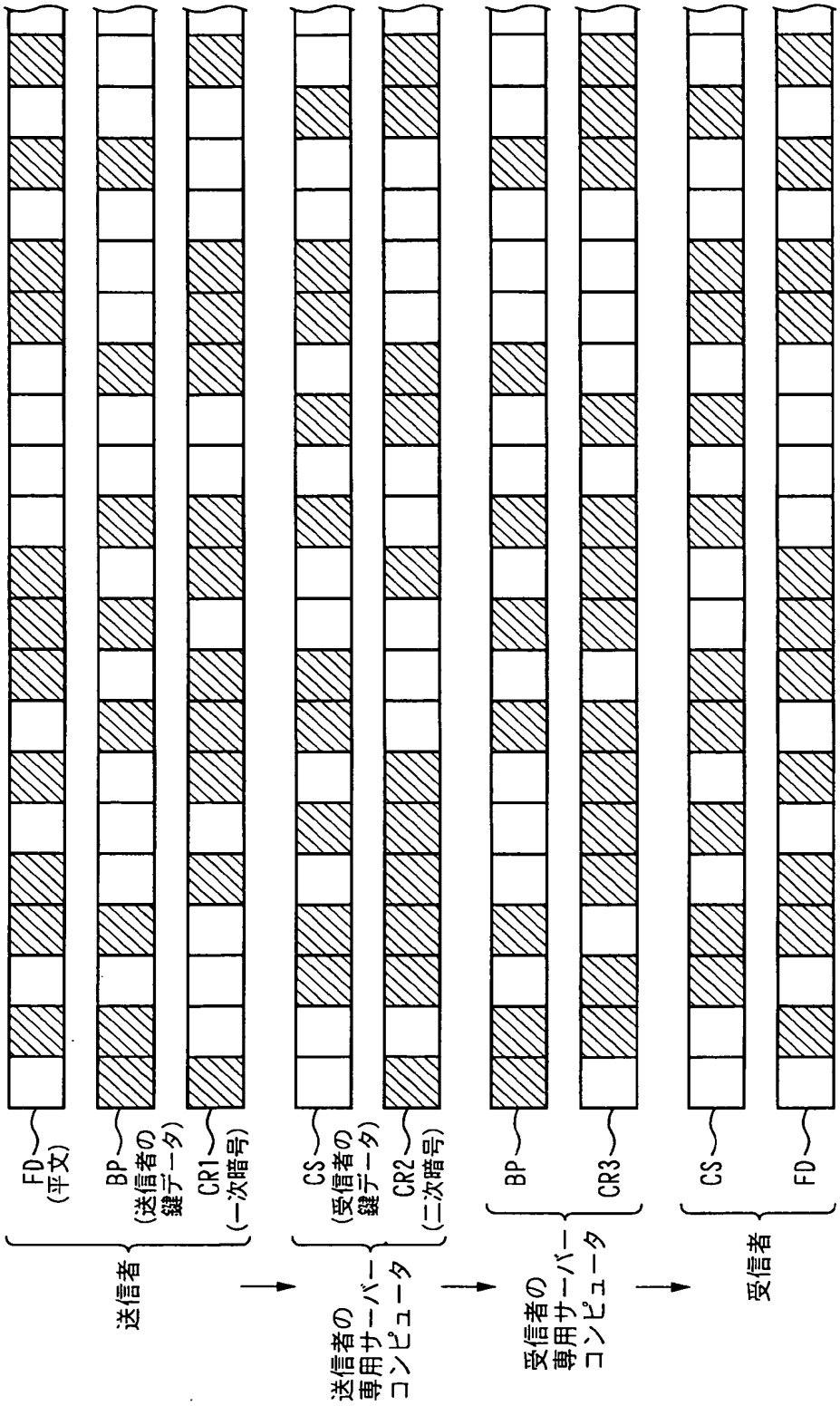
[図1]



[図2]

送信元	暗号状態	送信先
送信者(3)	一次暗号データ	送信者の専用サーバー(5A)
送信者の専用サーバー(5A)	受信者の鍵データなど問合せ	データセンターのサーバー(2A)
送信者の専用サーバー(5A)	二次暗号データ	受信者の専用サーバー(6)
受信者の専用サーバー(6)	送信者の鍵データなど問合せ	データセンターのサーバー(2A)
受信者の専用サーバー(6)	三次暗号データ	受信者(4)

[図3]


FD
(平文)
BP
(送信者の
鍵データ)
CR1
(一次暗号)
送信者
CS
(受信者の
鍵データ)
CR2
(二次暗号)
送信者の
専用サーバー
コンピュータ
BP
CR3
受信者の
専用サーバー
コンピュータ
CS
FD
受信者

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/015493

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/20, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/20, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-250059 A (International Business Machines Corp.), 26 September, 1995 (26.09.95), Par. Nos. [0002] to [0005] & EP 669741 A & US 5479514 A	1,3-8,10,11
Y	JP 7-245605 A (Fujitsu Ltd.), 19 September, 1995 (19.09.95), Par. Nos. [0020] to [0026]; Fig. 1 & GB 2287160 A & US 5642420 A	1,3-8,10,11
A	JP 2002-9758 A (Kabushiki Kaisha Isoppu), 11 January, 2002 (11.01.02), Par. Nos. [0012] to [0025]; Fig. 1 (Family: none)	2,9

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 November, 2004 (17.11.04)	07 December, 2004 (07.12.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/015493

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-204323 A (Yasumasa UYAMA), 18 July, 2003 (18.07.03), Par. Nos. [0117] to [0125]; Fig. 14 & US 2002-126848 A & EP 1244267 A	2,9
Y	JP 9-153014 A (Meteora System Kabushiki Kaisha), 10 June, 1997 (10.06.97), Full text (Family: none)	4,6,7
Y	JP 2001-217825 A (Victor Company Of Japan, Ltd.), 10 August, 2001 (10.08.01), Full text; Fig. 1 (Family: none)	6,7
Y	JP 2000-183866 A (Nippon Telegraph And Telephone Corp.), 30 June, 2000 (30.06.00), Full text; Fig. 3 (Family: none)	8-11

国際調査報告

国際出願番号　PCT／JP2004／015493

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／20, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／20, H04L9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 7－250059 A（インターナショナル・ビジネス・マシーンズ・コーポレイション）1995. 9. 26, 段落【0002】－【0005】& EP 669741 A & US 5479514 A	1, 3－8, 10, 11
Y	JP 7－245605 A（富士通株式会社）1995. 9. 19, 段落【0020】－【0026】, 図1 & GB 2287160 A & US 5642420 A	1, 3－8, 10, 11
A	JP 2002－9758 A（株式会社イソップ）2002.	2, 9

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　17. 11. 2004	国際調査報告の発送日　07.12.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　3574 青木　重徳 電話番号　03－3581－1101　内線　3597

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	１．１１，段落【００１２】－【００２５】，図１（ファミリーなし）	
Ａ	ＪＰ　２００３－２０４３２３　Ａ（宇山靖政）２００３．７．１８，段落【０１１７】－【０１２５】，図１４　＆　ＵＳ　２００２－１２６８４８　Ａ　＆　ＥＰ　１２４４２６７　Ａ	２，９
Ｙ	ＪＰ　９－１５３０１４　Ａ（メテオーラ・システム株式会社）１９９７．６．１０，全文（ファミリーなし）	４，６，７
Ｙ	ＪＰ　２００１－２１７８２５　Ａ（日本ビクター株式会社）２００１．８．１０，全文，図１（ファミリーなし）	６，７
Ｙ	ＪＰ　２０００－１８３８６６　Ａ（日本電信電話株式会社）２０００．６．３０，全文，図３（ファミリーなし）	８－１１

第Ⅳ欄　要約（第１ページの５の続き）

送信者はデータを自己の鍵で暗号化し、データセンター２に送る。データセンター２は、暗号化データを送信者の鍵を使って復号した後、受信者の鍵で再暗号化し、受信者４に送信する。受信者は自己の鍵でその再暗号化データを復号し、元のデータを得ることで、暗号化通信を行うことができる。尚、本発明で用いられる暗号アルゴリズムは平文と鍵とのビット単位ＸＯＲ演算である。